Amendments to the Specification

Please replace the paragraph on Page 16, beginning on line 2, with the following amended paragraph.

As a method of calculation, an addition chain method or the like is often adopted (refer to "Angouriron Nyuumon" ("E. Okamoto, An Introduction to the Theory of Cryptography, published by Kyoritsu shuppan on February 25, 1993 (pages 94-97)")); however, with such an algorithm processing speed is slow, and the time required for a transaction utilizing an IC card may exceed the user's allowable time. Therefore, it is the CRT to produce M from the result of a modular exponentiation for 2 prime factors, P and Q, of the public modulus N, instead of simply performing the modular exponentiation for X and N.